REMARKS/ARGUMENTS

The Examiner rejects claims 1, 3-7, 16, 23, and 25 under 35 U.S.C.§102(e) as being unpatentable over Hankinson et al. (U.S. 6,799,202); claims 2, 8, 9, 17, 18, 26-36 under 35 U.S.C.§103(a) as being unpatentable over Hankinson et al. in view of Schmeidler (U.S. 6,763,370); claims 10-12 and 37 under Section 103(a) as being unpatentable over Hankinson-Schmeidler in view of Kekic (U.S. 6,664,978); and claims 13-15, 19-22, and 24 under Section 103(a) as being unpatentable over Hankinson and further in view of Kekic.

Applicant respectfully traverses the Examiner's rejection. Applicants have canceled all of the pending claims and added new claims 38-76 of which claims 38, 53, and 69 are independent. Independent claims 38, 53, and 69 are patentable over the cited references for at least the features highlighted below in the claims:

> 38. An arrangement for serving information requests, comprising:
>
> a plurality of informational servers connected to a communications network, all of the informational servers having a common address on the communications network and serving a set of information to clients, each of the informational servers being configured to receive a transaction request associated with an individual transaction and to provide a response to each transaction request; and
>
> a content director connecting the informational servers to the communications network and distributing transaction requests among the informational servers comprising:
>
> a flow switch that parses plain text transaction requests to locate selected fields, selects an appropriate informational server to service each transaction request, and thereafter forwards at least portions of the parsed transaction requests to a selected one of the informational servers; and
>
> a cryptographic module that decrypts, *prior to parsing and informational server selection by the flow switch,* cipher text transaction requests and provides plain text transaction requests to the flow switch, *wherein, prior to decryption, the cipher text transaction requests have not been routed by another flow switch.*
>
> 53. In an arrangement comprising a plurality of informational servers connected to a communications network, all of the informational servers having a common address on the communications network and serving a set of information to clients, each of the informational servers being configured to receive a transaction

request associated with an individual transaction and to provide a response to each transaction request, a method for serving transaction requests from clients, comprising:

a cryptographic module decrypting a cipher text transaction request to provide a plain text transaction request to a first flow switch;

the first flow switch parsing the plain text transaction request to locate one or more selected fields;

the first flow switch, based on the one or more selected fields, selecting an appropriate informational server to service the transaction request; and

the first flow switch thereafter forwarding at least portions of the plain text transaction request to a selected one of the informational servers, *wherein the cipher text transaction request is decrypted prior to the parsing and selecting steps and wherein, prior to the decrypting step, the cipher text transaction request has not been directed to a flow switch other than the first flow switch.*

69. An arrangement for serving information requests, comprising:

a plurality of informational servers connected to a communications network, all of the informational servers having a common address on the communications network and serving a set of information to clients, each of the informational servers being configured to receive a transaction request associated with an individual transaction and to provide a response to each transaction request; and

a content director connecting the informational servers to the communications network and distributing transaction requests among the informational servers comprising:

first flow switching means for parsing plain text transaction requests to locate selected fields, selecting an appropriate informational server to service each transaction request, and thereafter forwarding at least portions of the parsed transaction requests to a selected one of the informational servers;

decrypting means for decrypting, *prior to parsing and informational server selection by the first flow switching means,* cipher text transaction requests and providing plain text transaction requests to the first flow switching means, *wherein, prior to the decrypting function, the cipher text transaction request has not been directed to a flow switching means other than the first flow switching means.*

Conventional web switches have difficulty maintaining transaction coherency when a communication session with a client transitions from plain text (unsecured) to encrypted (secure) modes. To protect client/server communications from eavesdropping, tampering and message forgery, the Secure Sockets Layer (SSL) protocol is used to transport secured messages. The cookie

in encrypted communications is also encrypted. When a transaction transitions from plain to cipher text, a new session ID is assigned to the transaction. Because the payload of the packet is encrypted, web switches assume that the next packet received from an IP address after the transaction becomes encrypted is a part of the immediately preceding clear text session with the same IP address. This assumption is not always correct. Many users, such as users behind a firewall or subscribers to an internet service such as Megaproxy™ offered by America On Line, can have the same global IP address. The encrypted sessions of such users can be crossed by the web switch, resulting in customer dissatisfaction and lost business. Web switches can also require excessive amounts of computational resources and otherwise suffer from computational inefficiencies.

The present invention can overcome this problem by positioning a cryptographic module between the communications network and the IP switch to selectively trans-crypt data within a secure HTTP transaction between a client and the network flow switch. The cryptographic module decrypts the packet before the packet is otherwise processed (*e.g.,* parsed) by the network flow switch and thereby identifies embedded destination and/or source invariants in the cipher text portion of the packet. Frequently requested content can thereby be efficiently segregated and cached even among a cluster configuration of network flow switches.

Hankinson et al.

Hankinson et al. is directed to a high speed server in which different functions of the server's state machine are distributed across a plurality of processors running a plurality of operating systems. The web server has a number of members categorized into member classes. Each member class has a distinct specialized operating system that is optimized for its function. Load balancing (such as is performed by a traffic manager prior to routing by the flow switch) is performed without regard to the message contents prior to transmission of a message to a dispatcher 720 (col. 17, lines 41-50). With reference to Fig. 7 and col. 21, line 64-col. 22, line 8, an encrypted message is transferred from a receiver 745 (or input) to a dispatcher (or switch) 720. Dispatcher 720 then sends the message to another dispatcher 725 over a private connection 730. Dispatcher 725 then sends the message to a decoder 735, which decodes the message and returns the decoded message to dispatcher 725.

Dispatcher 725 then sends a message identifying the location of the requested data to one of responders 740, and the responder 740 retrieves and sends the information to a decoder 735 for encryption and subsequently forwards an encrypted response, containing the encrypted information, to the client.

Hankinson et al. teaches the routing of the encrypted message first from a receiver 745 (which performs an initial analysis of the message col. 29, lines 33-37) to a first dispatcher 720 and second from a first dispatcher 720 to a second dispatcher 725 *before the message is decrypted.* In contrast, the claimed invention decrypts the message before it is initially routed by a switch, such as the receiver. Accordingly, Hankinson et al. fails to address the problem noted above, namely how to distinguish transaction requests from different clients having a common address on the communications network.

The remaining references fail to overcome the deficiencies of Hankinson et al.

Schmeidler et al.

Schmeidler et al. is directed to a system for secure delivery of on-demand content over broadband access networks that uses servers and security mechanisms to prevent client processes from accessing and executing content without authorization. A briq is mapped into a directory and file where it is stored in memory. In this manner, file system 1008 functions as an interface between the network request from the SCDP system and the memory 1050. Fig. 12 diagrams a briq. A briq 1200 includes a briq header 1202, a cryptoblock 1204, a superblock 1206, and one or more titles 1208A-N. A URN is a unique identifier of a title within a briq. The URN can correspond exactly to the current location of the title in the vendor's storage server. A URL identifies the current location of the briq in a RAFT storage server.

Kekic et al.

Kekic et al. is directed to a client-server management system using a combination of event rules and an event engine. In response to a selected event, a predetermined management action is undertaken.

Accordingly, the pending claims are allowable.

The dependent claims provide further reasons for allowability over the cited references.

By way of example, dependent claims 39, 54, and 70 are directed to the simultaneous or near simultaneous receipt of encrypted transaction requests from different clients having a common electronic address on the network.

Dependent claims 40, 44, 45, 55, 59-60, 71, and 74 are directed to a hot invariant table identifying information frequently requested from informational servers.

Dependent claims 42-43, 46, 57-58, 61, 72, and 75 are directed to the use of a digest value, for frequently requested information, to point to a location in the hot invariant table where objects regarding the information are stored. Although hashing is referenced at col. 18, lines 44-51, of Schmeidler, the hash code and an encryption key are used to digitally sign a launch string. The hash code is not related to a stored location of an object.

Dependent claims 49-52, 64-68, and 76 are directed to the switch tagging responses being forwarded to clients.

Based upon the foregoing, Applicants believe that all pending claims are in condition for allowance and such disposition is respectfully requested. In the event that a telephone conversation would further prosecution and/or expedite allowance, the Examiner is invited to contact the undersigned.

Respectfully submitted,

SHERIDAN ROSS P.C.

By: Douglas Swartz

Douglas W. Swartz
Registration No. 37,739
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700

Date: Feb. 21, 2005